REMARKS

Applicant has carefully reviewed and considered the final Office Action mailed on March 12, 2007, and the references cited therewith. Claims 1-20 are pending in this application.

Claims 1 and 13 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Claims 1-3 and 13-18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over WO2001/26322 to Khalil et al. (hereinafter Khalil) in view of U.S. Patent No. 6,948,074 to Borella et al. (hereinafter Borella) in still further view of U.S. Patent Application No. 2001/0016492 to Igarashi et al. (hereinafter Igarashi). Claims 4-7 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Khalil in view of Borella in still further view of Igarashi, and further in view of U.S. Patent Application No. 2002/0062385 to Dowling et al. (hereinafter Dowling). Claims 8-12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Khalil in view of Borella in further view of Igarashi and in still further view of Dowling, and further in view of U.S. Patent No. 6,915,345 to Tummala et al. (hereinafter Tummala). Claims 19 and 20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Khalil in view of Borella in further view of Igarashi, and further in view of U.S. Patent No. 6,785,823 to Abrol et al. (hereinafter Abrol).

Applicant respectfully traverses the rejection of all pending claims, as the features of the claims are neither disclosed nor suggested by the cited references.

With regard to the rejection of claims 1 and 13 under 35 U.S.C. § 112, the Office Action states (Office Action mailed March 12, 2007, p. 3, par. 3):

> The added limitation, "send the Reg-Req message including the second at least one key ", in line 19-20 of claim 1 and "a first one of the plurality of the session keys is sent by the AAAH via the Reg-Req message", in lines 10-11 of claim 13 is considered new matter. The relaying of the Req-Req message from the AAAH to the AH is discussed on page 15, line 27 – page 16, line 2. The passage references the receipt of the Reg-Req message and generates session keys and distributing the session keys are "in a secure fashion", but does not state that any session key is included in the Reg-Req message that is sent to the HA.

With regard to the rejection of claims 1 and 13 under 35 U.S.C. § 112, Applicant respectfully submits that independent claim 1 recites:

1. (Previously Presented) A system for a secure key distribution protocol in AAA for Mobile IP, comprising:

an MN that is configured to: generate a Reg-Req message that includes Diffie-Hellman parameters that are used to generate session keys and produce signatures; initiate an authentication session by sending the Reg-Req message; receive a Reg-Reply message that includes session keys that may be used to directly communicate with the AAAH, AAAF, HA, and FA nodes while the MN is in a foreign authority, wherein the session keys are encrypted and wherein the session keys include a first at least one key, a second at least one key, and a third at least one key;

an FA that is configured to: receive the Reg-Req message; ensure that the authentication session is valid; and when valid, sign and send the Reg-Req message; otherwise, end the authentication session; receive, and authenticate the Reg-Reply message, decrypt at least one key of the session keys; sign, and send the Reg-Reply message to the MN;

an AAAF that is configured to: receive and authenticate the Reg-Req message; generate a first at least one key of the session keys using the Diffie-Hellman algorithm and the Diffie-Hellman parameters; add an identifier relating to the Reg-Req message; sign and send the Reg-Req message; receive, authenticate, sign and send the Reg-Reply message to the FA;

an AAAH that is configured to: receive and authenticate the Reg-Req message; generate a second at least one key of the session keys; sign and send the Reg-Req message including the second at least one key; receive and authenticate the Reg-Reply message; generate a third at least one key of the session keys; encrypt the session keys; sign and send the Reg-Reply message including the third at least one key to the AAAF; and

an HA that is configured to: receive the Reg-Req message including the second at least one key; prepare a Reg-Reply message in response to the Reg-Req message; and send the Reg-Reply message to the AAAH.

The Office Action states (Office Action mailed March 12, 2007, p. 3, par. 3):

The added limitation, "send the Reg-Req message including the second at least one key ", in line 19-20 of claim 1 and "a first one of the plurality of the session keys is sent by the AAAH via the Reg-Req message", in lines 10-11 of claim 13 is considered new matter. The relaying of the Req-Req message from the AAAH to the AH is discussed on page 15, line 27 – page 16, line 2. The passage references the receipt of the Reg-Req message and generates session keys and distributing the session keys are "in a secure fashion", but does not state that any session key is included in the Reg-Req message that is sent to the HA.

Applicant respectfully submits that claim 1 recites an AAAH that is configured to "sign and send the Reg-Req message including the second at least one key." The specification, on

page 15, line 27 – page 16, line 2 discusses an example embodiment wherein the AAAH 525 generates session keys for FA, HA, and MN, "which are distributed in a secure fashion," and then discusses the encryption of the session keys $K_{HA\text{-}FA}$ and $K_{FA\text{-}HA}$ by the AAAH 525 using the SA between the AAAH 525 and the HA 530. On page 16, lines 1-2 the specification discusses the AAAH 525 forwarding the Reg-Req message 550 to the AH. Fig. 5 illustrates an example Reg-Req message 550 that is sent by the AAAH 525 to the HA 530, which includes at least the session key $K_{HA\text{-}FA}$ encrypted using $K_{AAAH\text{-}HA}$. Further, the specification, page 16, lines 5-6 states:

> Message 550 is received by HA 530. HA 530 then registers MN 510's current location, and stores the two session keys received from the AAAH 525. HA 530 then generates reply message 555, signs the message using $AUTH_{HA\text{-}AAAH}$, and sends reply message 555 to AAAH 525.

An example distribution of the session keys by the AAAH 525 is discussed further by the specification at page 16, lines 7-13 (*See also* Fig. 5, messages 555, 560):

> AAAH 525 receives message 555 sent by HA 530. After authenticating Reg-Reply message 555, AAAH 525 adds session keys $K_{FA\text{-}MN}$, $K_{MN\text{-}HA}$, $K_{MN\text{-}AAAF}$ and newly created key $K_{AAAH\text{-}AAAF}$ to the message. Keys $K_{FA\text{-}MN}$, $K_{FA\text{-}HA}$, and $K_{AAAH\text{-}AAAF}$ are encrypted using the old key $K_{AAAH\text{-}AAAF}$. AAAH also adds keys $K_{MN\text{-}FA}$, $K_{MN\text{-}HA}$, and $K_{MN\text{-}AAAF}$ to the message that are encrypted using key $K_{MN\text{-}AAAH}$. AAAH 525 signs message 560 with signature $AUTH_{AAAH\text{-}AAAF}$ and sends message 560 to AAAF 520.

Thus, "sign and send the Reg-Req message including the second at least one key," as recited by independent claim 1, and "wherein a first one of the plurality of the session keys is sent by the AAAH via the Reg-Req message to the HA," as recited by independent claim 13, are fully supported by the specification. Therefore, applicant respectfully requests that the rejection of claims 1 and 13 under 35 U.S.C. § 112 be withdrawn.

With regard to the rejection of claims 1-3 and 13-18 under 35 U.S.C. § 103(a), Applicant respectfully submits that independent claim 1 recites, "an AAAH that is configured to: receive and authenticate the Reg-Req message; generate a second at least one key of the session keys; sign and send the Reg-Req message including the second at least one key; receive and authenticate the Reg-Reply message; generate a third at least one key of the session keys;

encrypt the session keys; sign and send the Reg-Reply message including the third at least one key to the AAAF."

In stark contrast, Khalil (per Abstract) is directed to a key exchange for a network architecture. A mobile node that roams over a foreign domain sends a registration request to a home domain using the foreign domain. The identity of the mobile node within the registration request is encrypted. The home domain receives the registration request and decrypts the mobile node identity. The home domain generates a registration reply that includes encryption keys for encrypting information to be transmitted between and among the home domain, the foreign domain, and the mobile node.

The Office Action (pages 6-7, pars. l and o) cites Khalil at page 19, lines 12-23 as teaching "Generate a second at least one key of the session keys" and "Generate a third at least one key of the session keys." The Office Action (page 7, pars. s and t) further cites Khalil, figure 13d, as teaching "Prepare a Reg-Reply message in response to the Reg-Req message" and "Send the Reg-Reply message to the AAAH." However, these portions of Khalil merely discuss a home agent 1010 requesting a distribution center 1024 to generate three encryption keys, and to transmit the three encryption keys to the home agent for distribution to a mobile node 1002 and a foreign agent 1006. The home agent distributes the encryption keys to the foreign agent and the mobile node by generating a registration reply including keys 2 and 3 in unencrypted form and keys 1 and 3 in encrypted form. The home agent then transmits the registration reply to a server for further distribution to the foreign agent and mobile node. Thus, Khalil sends all the keys in one "registration reply" message.

In response to Applicant's previous arguments regarding Khalil's "distribution center," the Office action (page 2, par. 1) states:

> As to Applicant's argument that 'Khalil merely discusses a home agent requesting a distribution center to generate three encryption keys, and to transmit the three encryption keys to the home agent for distribution to a mobile node and a foreign agent", Applicant is directed to Khalil, page 17, lines 10-21 which states, "the home AAA server also provides the functionality of the key distribution center."

However, this brief mention by Khalil of the "functionality of the key distribution center" does not cure the deficiencies of Khalil with regard to the features recited by claims 1 and 13. A "registration request" is mentioned by Khalil at page 19, lines 3-11, but there is no mention of

sending any of the keys 1, 2, or 3 via the "registration request." Thus, Khalil does not teach or suggest "an AAAH" configured to "generate a second at least one key of the session keys; sign and send the Reg-Req message including the second at least one key" and "generate a third at least one key of the session keys; encrypt the session keys; sign and send the Reg-Reply message including the third at least one key to the AAAF" as recited by amended independent claim 1. Furthermore, Khalil does not teach or suggest "an HA that is configured to: receive the Reg-Req message including the second at least one key" as recited by amended independent claim 1.

Borella, directed to a method and system for distributed generation of unique random numbers, does not cure the deficiencies of Khalil in this regard. Moreover, Igarashi, directed to notifying a home agent via a foreign agent, an AAAF, and an AAAH, of location registration information transmitted from a mobile node, also fails to cure the deficiencies of Khalil. Furthermore, no reasonable combination of Khalil, Borella, or Igarashi cures the deficiencies of Khalil with regard to the recited features of amended independent claim 1 discussed above. Therefore, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

The rejection of dependent claims 2-3 should also be withdrawn for at least the same reasons as discussed above with regard to amended independent claim 1, as these claims recite additional features that are also not suggested or disclosed by the cited references.

Independent claim 13 recites, "wherein a first one of the plurality of the session keys is sent by the AAAH via the Reg-Req message to the HA, and wherein a second one of the plurality of the session keys is sent by the AAAH via the Reg-Reply message to the AAAF." The Office Action (page 8, item e) cites Igarashi, page 5, par. 130 as teaching "A first one of the plurality of the session keys is sent by the AAAH via the Reg-Req message to the HA." However, at par. 130, Igarishi states:

> Procedural step 5: The AAAH 100 extracts necessary information from the received AMR message, and performs the authentication of the mobile node 600. The AAAH 100 extracts, for example, a mobile node identifier (NAI: Network Access Identifier) from the AMR message, and accesses a service control database 300 by using the extracted identifier as a key. As a result, a user profile (service profile information) corresponding to the mobile node 600 is extracted. If the AAAH 100 successfully performs the authentication of the AMR message, it adds the above described service profile information to an HAR (registration request) message, and forwards the message to the home agent 200 via the IP network 80.

Applicant respectfully submits that there is no mention or suggestion of any "session key" being transmitted to the home agent 200 by the AAAH 100 of Igarishi. For reasons similar to those discussed previously with regard to claim 1, Applicant respectfully submits that the rejection of claim 13 should also be withdrawn, as the addition of Igarishi does not cure the deficiencies of Khalil discussed previously with regard to claim 1.

Similarly, the rejection of dependent claims 14-18, which depend either directly or indirectly from amended independent claim 13, should also be withdrawn for at least the same reasons as discussed above with regard to amended independent claim 13.

With regard to the rejections of dependent claims 4-7 and dependent claims 8-12, Applicant respectfully submits that neither the addition of Dowling nor the further addition of Tummala cure the deficiencies of Khalil, Borella, and Igarashi as discussed previously with regard to amended independent claim 1. Thus, the rejections of dependent claims 4-7 and 8-12 should also be withdrawn.

Regarding the rejection of dependent claims 19 and 20, which depend indirectly from amended independent claim 13, Applicant respectfully submits that the addition of Abrol does not cure the deficiencies of Khalil, Borella, or Igarashi discussed previously with regard to amended independent claim 13. Therefore, the rejection of claims 19 and 20 should also be withdrawn.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (202-470-6454) to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 50-3521 and references 0038-012001.

Respectfully submitted,

Brake Hughes Bellermann LLP
Customer Number 53666
202-470-6454

Date June 15, 2007

Margo Livesay, Ph.D.
Reg. No. 41,946